



**Texas Medicaid & Healthcare Partnership**

# **TXMedCentral Secure FTP Server**

**Trading Partner User Guide**

**Version 3.0  
August 3, 2018**



**Table of Contents**

<b>1.0 OVERVIEW .....</b>	<b>3</b>
<b>2.0 REGISTRATION / ATTESTATION.....</b>	<b>3</b>
<b>3.0 TRADING PARTNER/USER ROLES AND RESPONSIBILITIES .....</b>	<b>4</b>
<b>4.0 CONNECTIVITY .....</b>	<b>5</b>
<b>5.0 DIRECTORY STRUCTURE.....</b>	<b>6</b>
<b>6.0 PASSWORD ADMINISTRATION.....</b>	<b>10</b>
<b>7.0 PURGE SCHEDULE .....</b>	<b>11</b>
<b>8.0 CONTACT .....</b>	<b>11</b>
<b>9.0 TECHNICAL SUPPORT .....</b>	<b>12</b>
<b>10.0 APPENDIX A: TERMS AND ABBREVIATIONS .....</b>	<b>13</b>
<b>11.0 APPENDIX B: TXMEDCENTRAL INDIVIDUAL USER AGREEMENT FORM .....</b>	<b>15</b>
<b>12.0 APPENDIX C: TXMEDCENTRAL SYSTEM TO SYSTEM USER AGREEMENT FORM .....</b>	<b>22</b>
<b>13.0 APPENDIX D: CHANGE LOG .....</b>	<b>28</b>



## 1.0 OVERVIEW

The Texas Medicaid & Healthcare Partnership (TMHP) TXMedCentral server provides a secure method for Texas Medicaid and Children's Health Insurance Program (CHIP), Managed Care Organizations (MCOs), Texas Medicaid Administrative System (TMAS) contractors, and State Agencies to exchange interface files, memorandums and reports.

All individuals and organizations must have access to the Internet in order to connect to the TXMedCentral server.

The TXMedCentral secure FTP server is located at the hostname 'txmedcentral.tmhp.org' for the production environment, or 'txmedreg.tmhp.org' for regression. External users connecting only with a secure, encrypted protocol are able to connect.

## 2.0 REGISTRATION / ATTESTATION

Prior to creation of a user account, all users must attest that they will comply with the security procedures. All users must sign a user agreement attestation form (Appendix B or C) before a user ID is issued. In order for an attestation form to be considered complete, the user must provide data in all applicable fields on the document. Supervisor contact information and approval signature is required.

Separate attestations forms are required for access to Regression and Production. The regression environment is used only for directed testing – no production files should be sent to Regression.

After six consecutive invalid login attempts or 90 days of inactivity, the user ID will be systematically disabled. The user must contact the TXMedCentral Administrator ([TXMedCentralAdmin@tmhp.com](mailto:TXMedCentralAdmin@tmhp.com)) to reactivate his/her ID. The ID will be reactivated once the user's credentials are validated by the administrator.

Individual user accounts (with the exception of HHSC, IG and TMHP accounts) will be permanently deleted after 120 days of inactivity. Users with deleted accounts will need to restart the process and fax in a new user agreement attestation form to TXMedCentral Administration.

HHSC, IG and TMHP will need to follow their normal processes for modifying corresponding Team Member Requests (TMRs) at TMHP to delete access from TXMedCentral.

***See Appendices B and C for attestation forms and instructions.***

### 3.0 TRADING PARTNER/USER ROLES AND RESPONSIBILITIES

The Trading Partner/user or the user's supervisor must notify the TXMedCentral Administrator and/or the EFT Administrator of any necessary account changes. Scheduling future changes to an account is preferred. Once the administrator is notified of the requested change, the administrator will update, or schedule an update, to the user's account.

Immediately upon identifying a risk for terminated user or possible compromise of user's account, notify [TXMedCentralAdmin@tmhp.com](mailto:TXMedCentralAdmin@tmhp.com) and [DL-EFTServerAdmins@tmhp.com](mailto:DL-EFTServerAdmins@tmhp.com) via email with "Urgent" in the subject line and/or "High Importance" classification. When these type of requests are properly labeled, TMHP will process them within 1 hour during business hours or otherwise no later than 1 business day from request when email notification is received.

The following are examples of the necessary notifications to TMHP. When scheduling more than 2 business days in advance, no urgency on the email is necessary.

- Possible integrity and/or security of user account:  
The Trading Partner/User must immediately notify the TXMedCentral Administrator if the Trading Partner/User suspects the integrity and/or security of the TXMedCentral user account may have been compromised. Suspected misuse or failure to make proper notification of changes will result in account termination.
- Employee terminations:  
Supervisor must immediately report employee terminations since confidential data on TXMedCentral is at risk of being compromised. The supervisor must send an e-mail within one business day at the latest.
- User account permission changes:  
The change may include adding or removing permissions or disabling the user accounts. A change in job duties that requires removal of access must be reported within one business day. Changes involving multiple accounts such as third party contract terminations should be emailed to the TXMedCentral Administrator at least 10 business days prior to the change.

It is the Trading Partner's/User's responsibility to notify the TXMedCentral Administrator up to 10 business days following any changes *not* associated to any risk, such as:

- Change in email address(es),
- Change of contact name(s),
- Change of phone number

Notification of changes in External Source IP address(es) of Trading Partner's secure file transfer host (applicable to System-to-System account types) must be emailed to [DL-EFTServerAdmins@tmhp.com](mailto:DL-EFTServerAdmins@tmhp.com).



## 4.0 CONNECTIVITY

There are two different sites for TXMedCentral – one for Production and one for testing (known as Regression).

- **Production** - The TXMedCentral Production SFTP server is available 23x7, all hours except 3:00-4:00 AM Mon-Sun and other approved maintenance windows. The host name of the server is **txmedcentral.tmhp.org**.
- **Regression** - The TXMedCentral Regression SFTP server is available Monday through Friday 8:00 am to 6:00 pm. The host name of the server is **txmedreg.tmhp.org**.

TMHP's TXMedCentral server environment operates on a Globalscape EFT Server Enterprise managed file transfer software platform behind a separate Globalscape DMZ Gateway, both on Windows Server OS platforms. TXMedCentral is periodically upgraded/patched to leverage enhancements, fixes, and maintain vendor support according to industry, TMHP, and external audit-directed standards and best practices for its secure file transfer environment. TXMedCentral fully audits/logs all secure file transfer activity of the connected accounts.

Only certain secure/encrypted protocols (see below) are supported by TXMedCentral (Production and Regression) servers. Users will not be able to connect to these secure file transfer servers using an unsecured FTP protocol.

TXMedCentral Individual user account types may utilize a standalone secure file transfer client program to connect to the TXMedCentral system. Although TMHP does not require any particular secure file transfer client program, it is recommended to use up-to-date and industry-standard secure file transfer programs. Individual user accounts may also utilize the <https://txmedcentral.tmhp.org> or <https://txmedreg.tmhp.org> webpages for file transfers.

The current versions of secure file transfer clients known to work with the TXMedCentral system include, but are not limited to:

- [CuteFTP](#)
- [WS FTP](#)
- [FileZilla](#)
- [CoreFTP/CoreFTP LE](#)
- [WinSCP](#)

To connect to TXMedCentral, software must be configured to:

- Point to the DNS (Domain Name System) name
- Use the supported protocol(s)
- Use passive mode when using FTPS (FTP over TLS/SSL) (the passive ports are 4000 to 4200, additional setup may be needed to open up access to these ports through your firewall)

Individual account clients must be able to connect to TXMedCentral using the protocols listed below.

- SFTP (SSH File Transfer Protocol) on port 22
- FTPS (FTP over TLS/SSL) in Explicit mode (AUTH TLS) on port 21
- FTPS (FTP over TLS/SSL) in Implicit mode on port 990

NOTE: If using one of the FTPS protocols (*not SFTP*), ensure you are connecting in “ftp passive” mode. The passive ports are 4000 to 4200. Additional setup *may* be needed by your network administrator to open up access to these ports through your firewall.

TXMedCentral System to System account types are intended for *connections coming from a trading partner’s system using a host-grade, vendor supported secure file transfer software that will use automated processes to interact with TMHP*. The External Partner must ensure the solution they implement on their secure file transfer host is fully adherent to industry standards and technical specifications for reliable managed secure file transfer operation and audits/logs all of External Partner’s side of file transfer activity between the External Partner and TMHP. TMHP cannot recommend any particular secure file transfer solution for an External Partner. It is advised that the grade of secure file transfer software used by the External Partner’s connecting server is properly administered and is comparable in class of features and security operation as the software architecture of TXMedCentral.

TXMedCentral System to System account types must be able to connect using the authentication method and only the *specific* protocol listed below.

- SFTP (SSH File Transfer Protocol) on port 22, using certificate (SSH public key) + expected IP address authentication
- The SSH public key file (.pub) must be supplied by the connecting partner to TMHP and associated to the system-to-system account. Please send the .pub file and the system-to-system account’s name to which it should be associated to TMHP’s EFT Server Admins team [DL-EFTServerAdmins@tmhp.com](mailto:DL-EFTServerAdmins@tmhp.com) and cc: the TXMedCentral administrator email box [TXMedCentralAdmin@tmhp.com](mailto:TXMedCentralAdmin@tmhp.com).

## 5.0 DIRECTORY STRUCTURE

TXMedCentral is host to other State agencies, interest groups and other users, but the primary users are the TMAS trading partners and the MCOs. These other users mentioned above may or may not have access to any of these particular directories. It depends upon their business need to access data on this server. The decision for granting access is left to Health and Human Services Commission (HHSC) and/or the TXMedCentral Administrators.

TMHP is the administrator of TXMedCentral. All requests to change or delete content on TXMedCentral must come through [TXMedCentralAdmin@tmhp.com](mailto:TXMedCentralAdmin@tmhp.com). All MCO users have download rights for all directories for which they have access. They also have access to upload files in directories assigned solely to the MCO (uploads to common directories will be reserved for TMHP, HHSC and MAXIMUS). MCOs will be responsible for updating their sub-contractors directory access by emailing add/remove requests to the TXMedCentral Administrators.



- Requests to delete files, add permissions for existing users, or add folders to profiles must be sent via email.
- Requests to add users must be accompanied by a new attestation via fax.
- Requests to add directories to a group's access must be initiated from HHSC.

When a new MCO is awarded a contract with HHSC to carry out managed care activities with TMHP, the Enrollment Broker, and other State Agencies, the TXMedCentral Administrator will assign a series of directories on TXMedCentral in order for the new plan to exchange files with all of the trading partners. Each MCO is appointed a 2-3 character acronym for their plan name and then a directory name follows. The assigned list of directories will include secure directories, restricted to the MCO, as well as access to directories assigned to most trading partners. Some additional directories could be added depending on additional business needs, e.g., STAR+Plus line of business.

Below is a list of current directories and their descriptions where the MCO acronym is designated by xxx. These folders exist within both the production and regression environments.

**xxx4800** – Directory used for STAR+Plus hearings information. TMHP, the STAR+Plus plan and HHSC have access to this folder.

**xxxARC** – Directory where the original files are archived after they are processed (in automated manner). TMHP and the MCO have access to this folder.

**xxxCBA** – Directory used for STAR+Plus Community Based Action decisions. TMHP, the STAR+Plus plan and HHSC have access to this folder.

**xxxCHIP** - If the MCO participates in the line of business, they will be assigned this directory. Contents of this directory will include CHIP enrollment files, CHIP provider files and CHIP vendor drug files. TMHP, the MCO, the Enrollment Broker, the Quality Monitor and HHSC have access to this folder.

**xxxCLM** – Directory used for to TMHP to upload 837 claim files for the MCO to adjudicate. TMHP and the MCO have access to this folder.

**xxxCSR** – Directory designated for the Claims Summary Reports (CSR). This directory is used for HHSC to download the MCO's CSR. TMHP, the MCO designated individual, and HHSC have access to this folder.

**xxxDecisions** – Directory used for STAR+Plus hearings information. TMHP, the STAR+Plus plan and HHSC have access to this folder.

**xxxDELIV** – Directory where the MCO deliverables are posted for HHSC. TMHP, the MCO and HHSC have access to this folder.

**xxxDTS** – Directory where the MCO places reports/deliverables for the Deliverables Tracking System (DTS) for HHSC. TMHP, the MCO and HHSC have access to this folder.

**xxxEMAIL** – Because the Protected Health Information (PHI) can no longer be emailed between the health plans and other trading partners, this directory was created to inquire about eligibility issues with the Enrollment Broker, HHSC and/or TMHP. TMHP, the MCO, the Enrollment Broker and HHSC have access to this folder.

**xxxENC** – Directory where the plan will drop encounter and 278 files. TMHP and the MCO have access to this folder.

**xxxENCTEST** – Directory where the plan will drop encounter files when directed by TMHP or HHSC. TMHP and the MCO have access to this folder.





**xxxFSR** - Directory designated for the Financial Summary Reports (FSR). This directory is used for HHSC to download the MCO's FSR. TMHP, the MCO, and HHSC have access to this folder.

**xxxGENL** – Directory where the plan uploads/downloads interfaces between them and TMHP. This folder can contain files such as processed claims, third party insurance, client on review, and SK-SAI files/response. TMHP and the MCO have access to this folder.

**xxxHC** – Directory for information related to Rural Health Center (RHC) and Federally Qualified Health Center (FQHC) activities. TMHP, the MCO and HHSC have access to this folder.

**xxxHearNotices** – Directory used for STAR+Plus hearings information. TMHP, the STAR+Plus plan and HHSC have access to this folder.

**xxxISP** – Directory used for submittals of STAR+Plus Waiver Individual Service Plans. TMHP, the STAR+Plus plan and HHSC have access to this folder.

**xxxLIB** – Directory where the plan uploads/downloads interfaces between them and the Enrollment Broker. See the EB-CHIPJIP for specific file information. This directory also contains the STAR/STAR+Plus vendor drug files. TMHP, the MCO, HHSC, and the Enrollment Broker have access to this directory.

**xxxMA** – Directory for Medicare Advantage Plans to place enrollment files. Not all plans will have this directory. TMHP, the MCO, and HHSC have access to this folder.

**xxxRR** – Directory designated for the production readiness review with the readiness review contractor. TMHP, the MCO, HHSC and the contractor have access to this folder.

**xxxRSP** – Directory for the MCO to upload X12 999, TA1, and 277CA response files for their processed 837 claim files retrieved from the xxxCLM folder. TMHP and the MCO have access to this folder.

**xxxSKISP** – Directory used for submittals of STAR Kids Individual Service Plans. TMHP, the STAR Kids plan, and HHSC have access to this folder.

**xxxSPW** – Directory used for notifications of STAR+Plus Waiver Action decisions. TMHP, the STAR+Plus plan and HHSC have access to this folder.

**xxxSuppDoc** – Directory for STAR+Plus hearings. TMHP the STAR+Plus plan and HHSC have access to this folder.

**C21JIP** – Directory where the TMHP Joint Interface Plan (JIP) is stored. This directory contains file layouts for the MCOs and other managed care trading partners. For more information on the JIPs, see the MCOJIPGU\*.doc stored in this folder. Most TXMedCentral users have access to this folder.

**C21VALUE** – Directory where the field values for the JIP are stored. The MCO layouts reference which value list to use for particular fields. Most TXMedCentral users have access to this folder.

**CHIPGENL** – Directory used for CHIP general announcements, meeting agendas, process/procedures, MCO scan call agendas/minutes and MCO Communication plan are stored. TMHP, all CHIP MCOs, HHSC and most CHIP trading partners have access to this folder.

**MCODATA** - Directory containing provider files generated from Compass21 and the Insurance Company file. TMHP, HHSC, MCOs and most trading partners have access to this folder.

**MCOGENL** – Directory used for the general communication from TMHP and HHSC to the MCOs. The Enrollment Broker Calendar is also stored in this folder. TMHP, HHSC, all MCOs and most trading partners have access to this folder.





**MCOLAYUT** – Directory used to store MCO file layouts and companion guides. This directory mostly contains file specifications as used by the Enrollment Broker and TMHP. TMHP, HHSC, the MCOs and most trading partners have access to this folder.

**MCOREFS** – Directory where the TMHP reference files are uploaded. These files include procedure code files, diagnosis code files, DRG code files, fee schedules, etc. See the MCOJIP Guide (C21JIP) for file names and delivery schedule. TMHP, HHSC, and the MCOs have access to this folder.

This list of folders may change over time. Generally, any additional folders or direction to delete folders will come from HHSC or as a result of a new business need.

## 6.0 PASSWORD ADMINISTRATION

After receiving a completed user agreement attestation form, the initial user ID and temporary password will be emailed to the user. The first time a login is initiated to the system, it will require the user to change the temporary password. If the attestation form is submitted and the user has not received the username and temporary password within five business days, the user may send an inquiry to the email address [TXMedCentralAdmin@tmhp.com](mailto:TXMedCentralAdmin@tmhp.com) for status.

### **Individual User:**

Passwords will expire every 90 calendar days – an email reminder will be sent out by TMHP seven (7) days prior to the expiration to notify the user to log in and change their password. Another email is sent out on the 90<sup>th</sup> day stating that the password has expired. To change the password at any time, see *Password Reset Guidelines* for instructions.

Password standards and guidelines for Individual Users:

- All account passwords will have a minimum length of eight characters
- All account passwords must contain upper and lower case letters, numbers and special characters (e.g. a-z, A-Z, 0-9, !, #, \$, %)
- All account passwords cannot include any Standard English words
- All Individual and Administrator User account passwords will set to expire every 90 calendar days

### **System to System Accounts:**

System-to-System accounts are required to be secured using *two* simultaneous authentication security factors (SSH key authentication + access to username restricted to expected IP address). *Therefore, password-based authentication is not used by System-to-System accounts, and password resets are not applicable to System-to-System accounts.* The connecting partner's appropriate system personnel should generate and provide an SSH public user key they would like associated for access to a particular system-to-system account. The generated SSH user key shall *only* be used for authenticating to the system-to-system account, and TXMedCentral will *expire* the SSH user key in 2 years (730 days) aligning with TMHP SSH user key security policies. A copy of the TMHP SSH user key security policies can be obtained from TMHP's EFT Server Admins team [DL-EFTServerAdmins@tmhp.com](mailto:DL-EFTServerAdmins@tmhp.com) during authentication setup. Authentication setup for System-to-System accounts will be handled by TMHP's EFT Server Admins team in coordination with TMHP's TXMedCentral Admins team.

### **Password Reset Guidelines:**

TXMedCentral users have the ability to change their own password, within the password security standards and guidelines incorporated.



TXMedCentral Users who *need to change their password (almost or already expired)* should visit <https://txmedcentral.tmhp.org> for production, or <https://txmedreg.tmhp.org> for regression, and log in with their current username and password. After logging in, a password change screen will automatically appear. Users who *want (but don't need) to change their password* should log in to the website and click the “change password” option on the top of the screen.

TXMedCentral Users who have *forgotten their password* can visit <https://txmedcentral.tmhp.org> for production, or <https://txmedreg.tmhp.org> for regression, and click the “forgot password” link. They must provide their username and the correct email address associated with that username. Then they receive an email with an automatically generated link to use to create a new password.

For *manual password resets* (or for *disabled usernames*), TXMedCentral Users should email their requests to [TXMedCentralAdmin@tmhp.com](mailto:TXMedCentralAdmin@tmhp.com).

## 7.0 PURGE SCHEDULE

Files should be downloaded from TXMedCentral on a daily basis for MCO/trading partner use. In order to maintain space on TXMedCentral, files are automatically purged from most folders when the TXMedCentral modification dates are older than 90 days. Some exceptions to this rule are as follows:

- Files from the following folders are not on an automatic purge cycle: /MCOGENL, /C21JIP, /C21VALUE.
- Files from /xxxCLM and /xxxRSP will be purged with TXMedCentral modification dates older than 36 days.
- Files that will not be purged unless requested by HHSC are: xxxRR, xxx4800, xxxCBA, xxxDecisions, xxxHearNotices, xxxISP, xxxSKISP, xxxSPW, xxxSuppDoc.
- If the TXMedCentral administrator chooses to purge outside of the normal schedule, an email alert is generally sent out to all MCOs and TMAS partners.

**Note:** This is not a comprehensive list. Questions about directories not listed can be addressed to [TXMedCentralAdmin@tmhp.com](mailto:TXMedCentralAdmin@tmhp.com).

## 8.0 CONTACT

If the user encounters issues with the TXMedCentral, please send an email to: [TXMedCentralAdmin@tmhp.com](mailto:TXMedCentralAdmin@tmhp.com).

TXMedCentral Fax Number: (512) 506-6625



## 9.0 TECHNICAL SUPPORT

### **Individual (personal) Account Support:**

Individual User account support is provided by [TXMedCentralAdmin@tmhp.com](mailto:TXMedCentralAdmin@tmhp.com). Support is limited to permissions, password resets, and other file administration and business process issues. TMHP does not provide technical support for Secure FTP *client software* issues. All software issues should be routed through the software vendor or helpdesk of the company/organization that is initiating the connection to TXMedCentral. The technical support staff at the originating company/organization may contact TMHP to verify what are appropriate configuration settings for connectivity to TXMedCentral.

### **System-to-System Account Support:**

TMHP EFT Server Admins team [DL-EFTServerAdmins@tmhp.com](mailto:DL-EFTServerAdmins@tmhp.com) will provide support for setting up System-to-System username access. Further support is limited to assisting with resolution of connectivity issues and advising on appropriate configuration settings. TMHP does not provide support for any External Partner's software that is used to connect. Support for permissions, file administration, and business process issues is provided by [TXMedCentralAdmin@tmhp.com](mailto:TXMedCentralAdmin@tmhp.com).

For TXMedCentral support escalations, please email [TXMedCentralAdmin@tmhp.com](mailto:TXMedCentralAdmin@tmhp.com).

## 10.0 APPENDIX A: TERMS AND ABBREVIATIONS

Term	Definition
277CA	X12 Claims Acknowledgement Report
837	X12 Healthcare Claim
999	X12 Implementation Acknowledgement transaction set
EB-CHIPJIP	Enrollment Broker/Children's Health Insurance Program Joint Interface Plan
CHIP	Children's Health Insurance Program
CSR	Claims Summary Reports
DNS	Domain Name System
DTS	Deliverables Tracking System
EFT	Enhanced File Transfer
FTP	File Transfer Protocol
FSR	Financial Summary Reports
FTPS	File Transfer Protocol Software
HHSC	(Texas) Health and Human Services Commission
ID	Identification
IP	Internet Protocol
JIP	Joint Interface Plan
MCO	Managed Care Organization
PHI	Protected Health Information
Regression	Test environment used for directed trading partner testing – no production files exist in this environment
SFTP	Secure File Transfer Protocol
SK-SAI	STAR Kids Screening and Assessment Instrument
SSL	Secure Socket Layer
SSH	Secure Socket Shell
STAR	State of Texas Access Reform
STAR Kids	State of Texas Access Reform providing Medicaid benefits to individuals with disabilities under the age of twenty-one
STAR+Plus	State of Texas Access Reform Plus care for elderly, Medicare/Medicaid Dual Eligibles and Long Term Support Services (LTSS)
Submitter ID / Receiver ID	In this document, this refers to IDs used for the exchange of X12 files between MCOs and TMHP through TXMedCentral
System to System	Partner's host-grade, vendor-supported, secure file transfer software making automated transfers with TXMedCentral
TA1	X12 Interchange Acknowledgement Report
TLS	Transfer Layer Security
TXMedCentral	Texas Medicaid Network for Managed Care Trading Partners
TMAS	Texas Medicaid Administrative System
TMHP	Texas Medicaid & Healthcare Partnership



Trading Partner	Any non-TMHP organization (or individual) who accesses TXMedCentral
-----------------	---



## **11.0 APPENDIX B: TXMEDCENTRAL INDIVIDUAL USER AGREEMENT FORM**





## TXMedCentral Individual User Agreement

All sections of the TXMedCentral Individual User Agreement must be completed and accurate before the request can be processed and approved.

### Section 1: Trading Partner Representative Environment Information

Please provide the following information:

Environment Requested (Regression or Production): \_\_\_\_\_

### Section 2: Trading Partner Representative Information

Please provide the following information:

Trading Partner Agency/Company Name: \_\_\_\_\_

Trading Partner Representative First Name: \_\_\_\_\_ Last Name: \_\_\_\_\_

Trading Partner Representative E-mail Address: \_\_\_\_\_

Trading Partner Representative Telephone Number: \_\_\_\_\_

Affiliated Agency/Company Name: \_\_\_\_\_

#### Trading Partner Representative's Supervisor:

First Name: \_\_\_\_\_ Last Name: \_\_\_\_\_

Trading Partner Representative's Supervisor Contact E-mail Address: \_\_\_\_\_

Trading Partner Representative's Supervisor Contact Telephone Number: \_\_\_\_\_



### Section 3: Trading Partner Representative Security Questions

Please provide answers to the following security questions:

**Note: Do not share below security questions with supervisor.  
Attestation continued on following page.**

What is your favorite cartoon character? \_\_\_\_\_

What is your favorite food? \_\_\_\_\_

What is the name of the street you grew up on? \_\_\_\_\_



## Section 4: Trading Partner Representative Attestation

### Authorized Use

I understand and acknowledge that:

1. TXMedCentral.tmhp.org is to be used for official state-approved business.
2. TXMedCentral.tmhp.org is not for personal use.
3. HHS Agencies and Business Partners have a duty to protect TXMedCentral.tmhp.org data.
4. HHS Agencies have the right to monitor the use of TXMedCentral.tmhp.org by their employees and Business Partners.
5. HHS Agency employees and Business Partners have no right to expect privacy in their use of TXMedCentral.tmhp.org or in the content of their communications sent or stored on TXMedCentral.tmhp.org.

I agree that:

1. I will use TXMedCentral.tmhp.org only for official state-approved business.
2. I will not use TXMedCentral.tmhp.org for personal reasons.
3. My use of TXMedCentral.tmhp.org may be monitored in ways that will not be disclosed to me and may not be apparent to me at the time.

### Personal Security Identification Codes (User IDs and Passwords)

I understand and acknowledge that:

1. I will receive and will be required to use a personal security identification code (User ID and Password) to gain access to and to use TXMedCentral.tmhp.org.
2. My User ID and Password are security measures and must be used only by me.
3. I will be held personally responsible for any actions taken, or for any harm, loss, or adverse consequences arising from the use of my User ID and Password, including any unauthorized use by a third-party if such party gains access to my User ID and Password due to my negligence or misconduct.
4. Transactions initiated under my User ID and Password will be considered as having been authorized and electronically signed by me.

I agree that:

1. I will not disclose my password to anyone.
2. I am responsible for any actions taken or for any harm, loss, or adverse consequences arising from the use of my User ID and Password, including any unauthorized use by a third-party if such party gains access to my User ID and Password due to my negligence or misconduct.

### Access to Data

I understand and acknowledge that proper authorization is required for access to all data owned by HHS Agencies. Failure to comply with this agreement may result in the loss of access privileges to TXMedCentral.tmhp.org.

I agree that:

1. I will not attempt to access, alter, or misuse any data that I am not authorized to work with in the performance of my job duties.
2. I will take active steps to prevent others from obtaining access to HHS Agency data, such as by logging out of TXMedCentral.tmhp.org before leaving the workstation.
3. Failure to comply with this agreement may result in the loss of access privileges to TXMedCentral.tmhp.org.



**I attest to the accuracy of the information provided on this request and have read and understand the details of this request. I authorize the exchange of data as defined in this request.**

\_\_\_\_\_  
Signature of Trading Partner Representative

\_\_\_\_\_  
Trading Partner Representative Name  
(Please Print)

\_\_\_\_\_  
Job Title

\_\_\_\_\_  
Date

**By signing below, supervisor attests that the Trading Partner Representative listed above has a business need and approves access to TXMedCentral.**

\_\_\_\_\_  
Supervisor's Signature

\_\_\_\_\_  
Supervisor's Name  
(Please Print)

\_\_\_\_\_  
Job Title

\_\_\_\_\_  
Date

## **Section 5: Request Submission Instruction**

Before faxing this request, ensure that all required information is completely filled out and that the agreement is signed. Incomplete requests cannot be processed.

Please fax to: 1-512-506-6625

## **Section 6: Questions**

For questions about the TXMedCentral Individual User Agreement, please contact the TXMedCentral Administrator at: [TXMedCentralAdmin@tmhp.com](mailto:TXMedCentralAdmin@tmhp.com).



## Individual User Agreement Instructions

### Section 1: Trading Partner Representative Environment Information

Section One Field	Instruction
Environment Requested (Regression or Production)	Enter the environment permissions are being requested for. Choose either: <b>Regression</b> or <b>Production</b>

### Section 2: Trading Partner Representative Information

Section Two Field	Instruction
Trading Partner Agency/Company Name	Enter your Agency/Company Name
Trading Partner Representative First Name / Last Name	Enter User's Name
Trading Partner Representative E-mail Address	Enter User's company email address (non company accounts will not be accepted i.e. yahoo, hotmail, gmail)
Trading Partner Representative Telephone Number	Enter User's business phone number
Affiliated Agency/Company Name	If a subcontractor, enter the Company with whom you are contracted. For example, identify the Managed Care Organization.
Trading Partner Representative's Supervisor First / Last Name	Enter Supervisor's Name
Trading Partner Representative's Supervisor Contact E-mail Address	Enter Supervisor's company e-mail address
Trading Partner Representative's Supervisor Contact Telephone Number	Enter Supervisor's phone number

### Section 3: Trading Partner Representative Security Questions

Section Three Field	Instruction
What is your favorite cartoon character?	Enter your answer
What is your favorite food?	Enter your answer
What is the name of the street you grew up on?	Enter your answer

### Section 4: Trading Partner Representative Attestation

Section Four Field	Instruction
Signature of Trading Partner Representative	Sign that you are attesting to the accuracy of the information provided on this request and have read and understand the details of this request and that you authorize the exchange of data as defined in this request.
Trading Partner Representative Name	Print your name



Job Title	Enter your job title
Date	Enter date you signed form
Supervisor's Signature	By signing, supervisor attests that the Trading Partner Representative listed above has a business need and approves access to TXMedCentral.
Supervisor's Name	Supervisor's printed name
Supervisor's Job Title	Supervisor's job title
Date	Date the supervisor signed form

#### Section 5: Request Submission Instruction

Section Five Field	Instruction
Before faxing this request, ensure that all required information is completely filled out, and that the agreement is signed. Incomplete requests cannot be processed.	Submit Fax to: (512) 506-6625

#### Section 6: Questions

Section Six Field	Instruction
For questions about the TXMedCentral Individual User Agreement, please contact the TXMedCentral Administrator	Send email to: <a href="mailto:TXMedCentralAdmin@tmhp.com">TXMedCentralAdmin@tmhp.com</a>



## **12.0 APPENDIX C: TXMEDCENTRAL SYSTEM TO SYSTEM USER AGREEMENT FORM**





## TXMedCentral System to System User Agreement

All sections of the TXMedCentral System to System User Agreement must be completed and accurate before the request can be processed and approved.

### Section 1: Trading Partner Representative (SFTP System Administrator) Information

Please provide the following information:

Trading Partner Agency/Company Name: \_\_\_\_\_

Trading Partner Agency/Company Information Officer/Director Name: \_\_\_\_\_

Trading Partner Representative First Name: \_\_\_\_\_ Last Name: \_\_\_\_\_

Trading Partner Representative E-mail Address: \_\_\_\_\_

Trading Partner Representative Telephone Number: \_\_\_\_\_

Affiliated Agency/Company Name: \_\_\_\_\_

#### Trading Partner Representative's Supervisor :

First Name: \_\_\_\_\_ Last Name: \_\_\_\_\_

Trading Partner Representative's Supervisor E-mail Address: \_\_\_\_\_

Trading Partner Representative's Supervisor Telephone Number: \_\_\_\_\_

### Section 2: Trading Partner Representative System Information

Please provide the following information:

Environment Requested (Regression or Production): \_\_\_\_\_

Source External IP address(es) Please list each address:

\_\_\_\_\_

## Section 3: Trading Partner Representative Attestation

### Authorized Use

The organization understands and acknowledges that:

1. TXMedCentral.tmhp.org is to be used for official state-approved business.
2. HHS Agencies and Business Partners have a duty to protect TXMedCentral.tmhp.org data.
3. HHS Agencies have the right to monitor the use of TXMedCentral.tmhp.org by their employees and Business Partners.
4. HHS Agency employees and Business Partners have no right to expect privacy in their use of TXMedCentral.tmhp.org or in the content of their communications sent or stored on TXMedCentral.tmhp.org.

The Organization agrees that:

1. The organization will use TXMedCentral.tmhp.org only for official state-approved business.
2. The organization's use of TXMedCentral.tmhp.org may be monitored in ways that will not be disclosed to it and may not be apparent at the time.

### Security Identification Factors (System-to-System Username, SSH User Authentication Key, and External Source IP Address(es))

The organization understands and acknowledges that:

1. The organization will be required to use the Security Identification Factors (System-to-System Username, SSH User Authentication Key, and External Source IP Address(es)) to gain access to and to use TXMedCentral.tmhp.org or TXMedReg.tmhp.org.
2. The organization's System-to-System Username, SSH User Authentication Key, and External Source IP Address(es) are security measures and must be used only by the organization.
3. The organization will be held responsible for any actions taken, or for any harm, loss, or adverse consequences arising from the use of the System-to-System Username, SSH User Authentication Key, and External Source IP Address(es), including any unauthorized use by a third-party if such party gains access to the Security Identification Factors due to the organization's negligence or misconduct.
4. Transactions initiated under the organization's Security Identification Factors will be considered as having been authorized and electronically signed by the organization.

The organization agrees that:

1. The organization will not share possession or usage of the Security Identification Factors to anyone other than the specific IT system administrators who have been duly authorized to access TXMedCentral.tmhp.org accounts and files.
2. The organization is responsible for any actions taken or for any harm, loss, or adverse consequences arising from the use of the Security Identification Factors, including any unauthorized use by a third-party if such party gains access to the Security Identification Factors due to the organization's negligence or misconduct.

### Access to Data

The organization understands and acknowledges that proper authorization is required for access to all data owned by HHS Agencies. Failure to comply with this agreement may result in the loss of access privileges to TXMedCentral.tmhp.org.



I (we) attest to the accuracy of the information provided on this request and have read and understand the details of this request. I (we) authorize the exchange of data as defined in this request.

\_\_\_\_\_  
Signature of Trading Partner Representative

\_\_\_\_\_  
Trading Partner Representative Name  
(Please Print)

\_\_\_\_\_  
Job Title

\_\_\_\_\_  
Date

\_\_\_\_\_  
Supervisor's Signature

\_\_\_\_\_  
Supervisor's Name  
(Please Print)

\_\_\_\_\_  
Job Title

\_\_\_\_\_  
Date

## Section 4: Request Submission Instruction

Before faxing this request, ensure that all required information is completely filled out and that the agreement is signed. Incomplete requests cannot be processed.  
Please fax to: 1-512-506-6625

## Section 5: Questions

For questions about the TXMedCentral System to System User Agreement, please contact the TXMedCentral Administrator at: [TXMedCentralAdmin@tmhp.com](mailto:TXMedCentralAdmin@tmhp.com)



## System to System User Agreement Instructions

### Section 1: Trading Partner Representative Information:

Section One Field	Instruction
Trading Partner Agency/Company Name	Enter your Agency/Company Name
Trading Partner Agency/Company Information Officer/Director Name	Enter Agency/Company Information Officer / Director Name
Trading Partner Representative (SFTP System Administrator) First Name / Last Name	Enter your SFTP System Administrator's name who is the Representative for the system to system account
Trading Partner Representative E-mail Address	Enter Representative's company email address (non company accounts will not be accepted i.e. yahoo, hotmail, gmail)
Trading Partner Representative Telephone Number	Enter Representative's business phone number
Affiliated Agency/Company Name	If a subcontractor, enter the Company with whom you are contracted. For example, identify the Managed Care Organization.
Trading Partner Representative's Supervisor First / Last Name	Enter Supervisor's Name
Trading Partner Representative's Supervisor Contact E-mail Address	Enter Supervisor's company e-mail address
Trading Partner Representative's Supervisor Contact Telephone Number	Enter Supervisor's phone number

### Section 2: Trading Partner Representative System Information:

Section Two Field	Instruction
Environment Requested (Regression or Production)	Enter the environment permissions are being requested for. Choose either: <b>Regression</b> or <b>Production</b>
Source External IP address(es)	Enter the source external IP address(es) of the trading partner's secure file transfer host

### Section 3: Trading Partner Representative Attestation:

Section Three Field	Instruction
Signature of Trading Partner Representative	Sign that you are attesting to the accuracy of the information provided on this request and have read and understand the details of this request and that you authorize the exchange of data as defined in this request.
Trading Partner Representative Name	Print your name



Job Title	Enter your job title
Date	Enter date you signed form
Supervisor's Signature	By signing, supervisor attests that the Trading Partner Representative listed above has a business need and approves access to TXMedCentral.
Supervisor's Name	Supervisor's printed name
Supervisor's Job Title	Supervisor's job title
Date	Date the supervisor signed form

Section 4: Request Submission Instruction:

Section Four Field	Instruction
Before faxing this request, ensure that all required information is completely filled out, and that the agreement is signed. Incomplete requests cannot be processed.	Submit Fax to: (512) 506-6625

Section 5: Questions:

Section Five Field	Instruction
For questions about the TXMedCentral System to System User Agreement, please contact the TXMedCentral Administrator	Send email to: <a href="mailto:TXMedCentralAdmin@tmhp.com">TXMedCentralAdmin@tmhp.com</a>

## 13.0 APPENDIX D: CHANGE LOG

Change Date	Section Changed	Comments
7/21/2009	Connectivity	Clarification on SSH protocol for System to System Accounts
7/21/2009	Directory Structure	Clarification on user rights
1/18/2012	Overview	Clarification on the current state of TXMedCentral
1/18/2012	Registration / Attestation	Updated instructions for individual and system user agreements.
1/18/2012	Directory Structure	Modify current directory list
1/18/2012	Purge Schedule	Clarification on purging schedule; Updated Section #
1/18/2012	Terms & Abbreviations	Added additional terms to Terms & Abbreviations
1/18/2012	Appendix B	Added Section 1 & Modified Section #s
1/18/2012	Appendix C	Modified Section 3 to include new content
4/24/2014	Title Page	Title changed from "SFTP" to "Secure FTP Server"
4/24/2014	Overview	Minor changes detailing connectivity
4/24/2014	Connectivity	Description of EFT server added; replaced software versions with general instruction to use most current version; added additional FTPS instruction; added detailed instruction for system to system accounts
4/24/2014	Password Administration	Replaced system to system account password information with SSH key information; instructions added for resetting password; other minor description changes and hyperlinks updated
4/24/2014	Technical Support	Description changed from "user" account to "individual" account; defined the support team for each type of account
8/3/2018	Overview	Added regression hostname; removed requirement of using secure file transfer software
8/3/2018	Registration/Attestation	Added process of account deletion after 120 days of inactivity; added clarification to environment requested; moved attestation instructions to respective appendices B and C; corrected references to Appendix B and C
8/3/2018	Trading Partner/User Roles and Responsibilities	Added notice of IP address change to user responsibility; moved paragraph on account permission changes from Section 6.0



8/3/2018	Connectivity	Added additional web-based connection type; description changes for system-to-system accounts; removed IP addresses
8/3/2018	Directory Structure	Minor descriptive changes; removal of mco user permissions statement; updated description of directories: xxxENCTEST, xxxGENL, xxxLIB, xxxJIP, MCOGENL, MCOLAYUT, MCOREFS; removed xxxLTCHearing; added xxxSKISP
8/3/2018	Password Administration	Added SSH user key information to system-to-system account section; added regression links; removed unnecessary instruction for manual password resets; moved "Account Permission Change Guidelines" section to 3.0 Trading Partner/User Roles and Responsibilities
8/3/2018	Purge Schedule	Updated to include contact information for any folders not listed; removed folders no longer purged on monthly basis; updated wording to "TXMedCentral modification dates" instead of "create dates"; updated xxxCLM and xxxRSP to 36 days; added no purge cycle folders; added xxxSKISP and removed xxxLTCHearing
8/3/2018	Appendix A	Added terms: EFT, STAR Kids, SK-SAI, trading partner, and system to system
8/3/2018	Appendix B	Added fields for supervisor contact information and signature; moved instructions from Section 2.0; updated instruction fields to match attestation form
8/3/2018	Appendix C	Clarified Section 1 title and IP address field; removed submitter/receiver ID field from Section 2; updated Security Identification factors section to replace certificate and password with username, SSH key, and IP address, clarified agreement terms; updated instruction fields to match attestation form; added fields for supervisor contact information and signature